DOI 10.37882/2223-2966.2024.06.07

ВСТРАИВАНИЕ TIP В ЭКОСИСТЕМУ SOC

INTEGRATING TIP INTO THE SOC ECOSYSTEM

O. Borovskaya
I. Savelyev

Summary. The *purpose* of the work is to identify the benefits of using TI data and to create an approach to embedding TIP into the SOC ecosystem. The following research *methods* were used: consistent analysis of the mechanisms for using TI data, implying interaction with them at the time of receiving indicators of compromise in the system. The article categorizes and classifies TI data. The authors of the article analyzed the work experience of information security engineers specializing in the design and implementation of monitoring tools and response to information security incidents, which made it possible to apply practical skills in their work.
Research results: Categorization and classification of TI data was carried out. The practical significance of the study is confirmed by identifying the benefits of using TI data by integrating TIP with various solutions. The analysis showed that a successful strategy for choosing TI data is to diversify TI data from different manufacturers, since it is difficult to find one manufacturer that would completely cover the user's needs. Approaches to integrating TIP into the SOC ecosystem are described, as well as the main types of solutions in the context of reactive scenarios for using TI data.

Keywords: Threat Intelligence, Threat Intelligence Platform, TI data, indicators of compromise, SOC, analytics, alerting, enrichment, vulnerabilities, threats.

Боровская Ольга Евгеньевна
Финансовый университет при Правительстве Российской Федерации, г. Москва
borovskaya_olechka@mail.ru
Савельев Иван Андреевич
кандидат технических наук, доцент, Финансовый университет при Правительстве Российской Федерации, г. Москва
iasavelyev@fa.ru

Аннотация. *Цель работы* состоит в определении преимущества использования TI данных и создании подхода к встраиванию TIP в экосистему SOC.
Использовались следующие *методы исследования*: последовательный анализ механизмов использования TI данных, подразумевающих взаимодействие с ними в момент получения индикаторов компрометации в системе. В статье осуществляется категоризация и классификация TI данных. Авторами в статье проанализирован опыт работы инженеров по информационной безопасности (далее — ИБ), специализирующихся в области проектирования и внедрения средств мониторинга и реагирования на инциденты ИБ, что позволило применить в работе практические навыки.
Результаты исследования: проведена категоризация и классификация TI данных. Практическая значимость исследования подтверждается определением преимущества использования TI данных путем интеграции TIP с различными решениями. Анализ показал, что успешной стратегией выбора TI данных является диверсификация TI данных от различных производителей, поскольку сложно найти одного производителей, который полностью закрыл бы потребности пользователя. Описаны подходы к встраиванию TIP в экосистему SOC, а также основные типы решений в разрезе вариантов реактивных сценариев использования TI данных.

Ключевые слова: Threat Intelligence, Threat Intelligence Platform, TI данные, индикаторы компрометации, SOC, аналитика, алертинг, обогащение, уязвимости, угрозы.

Введение

Threat Intelligence (далее — TI) данные — это информация об актуальных ИБ-угрозах, содержащая тактики, техники и инструменты злоумышленников и позволяющая выстроить эффективную систему защиты [1].

Наиболее известными случаями хакерских атак в России за последние годы являются:

- атака на систему ЦБ России в 2021 г. (группировка MoneyTaker);
- мошенничество с 3-D Secure в 2021 г. (фишинг);
- атака на «Яндекс» в 2021 г. (DDoS-атака);
- атака на портал «Госуслуги» в 2022 г. (DDoS-атака);
- программы вымогатели Phobos, CryLock, Sojusz в 2022 г. (группировка OldGremlin);
- атака на «РЖД» в 2023 г. (DDoS-атака).

Знания тактик, техник и инструментов зловредных программ, используемых злоумышленниками, можно использовать в целях предотвращения дальнейших ИБ-угроз, защиты конечных точек и повышения уровень ИБ в Организации [2].

Постановка задачи

В рамках данной работы были поставлены следующие задачи:

- категорировать и классифицировать TI данные;
- выделить преимущества использования TI данных;
- определить направления назначения TI данных;
- сформировать реактивные сценарии использования TI данных;
- сформировать подход встраивания TIP в экосистему SOC;
- выделить особенности решений продуктов TI и TIP.

Категоризация TI данных

Существует несколько категорий TI данных:

— технические данные, которые включают в себя:
- уязвимости: данные о слабостях в ПО;
- сигнатуры вредоносных программ: уникальные строки кода;
- логи сетевой активности: события, происходящие в сети;
- конфигурационные файлы;
- списки IP- и URL-адресов.

— операционные данные, которые включают в себя:
- информация о новых вирусах и вредоносных программах;
- данные об инцидентах безопасности: тип атаки, методы, уязвимости;
- информация о действующих угрозах: сканирования уязвимостей, бот-атаки;
- данные об утечках данных: логины и пароли, персональные данные;
- информация о новых методах атак: социальная инженерия, фишинги.

— тактические данные, которые включают в себя:
- методы и тактики вредоносных программ: спам, взлом, фишинг, DDoS-атаки;
- данные о типах атак: SQL-инъекции, межсайтовый скриптинг, кликджекинг;
- методы защиты от конкретных угроз: конфигурация сети и ПО, обновление системы;
- информация о методах обнаружения и реагирования: инструменты мониторинга сетевой активности;
- данные о местоположении источников угроз: IP-адреса.

— стратегические данные, которые включают в себя:
- информация о группировках хакеров: намерения, цели и методы;
- географические данные о распространении угроз;
- информация об уязвимости ПО и слабым местам в системах;
- тенденции и прогнозы в кибербезопасности: предсказывание будущих угроз и принятие мер по их предотвращению;
- рекомендации по управлению рисками и методах реагирования на инциденты [3].

Выгоды от использования TI данных

Таким образом, выделяются следующие выгоды от использования TI данных:

— проактивная и реактивная защита;
— обнаружение угроз на более ранних этапах — более быстрое реагирование;
— ретроспективное обнаружение угроз;
— развитие системы защиты компании (без трудоемкого тестирования и внедрения);
— повышение уровня обеспечения ИБ.

Критерии выбора TI данных

Ключевыми критериями выбора TI данных различных производителей выступают:

— область покрытия (регионы, мир);
— отраслевая специфика (банки, промышленность, др.);
— состав данных (IP-, URL-адреса, Domains, Hash, Malware, APT, др.);
— полнота контекста (даты обнаружения, связанные индикаторы, данные whois, геопривязка, др.);
— актуальность (частота обновления);
— дополнительный инструментарий (отчетность, связи, др.);
— назначение TI данных (аналитика, алертинг, обогащение).

Успешной стратегией выбора TI данных является диверсификация TI данных от различных производителей, поскольку сложно найти одного производителей, который полностью закрыл бы потребности пользователя (отчеты Gartner, SANS) [4].

TI данных можно классифицировать следующим образом:

— по количеству индикаторов (по типам): «плоские» данные — IP- (v4, v6) и URL-адреса, Domain, Hash (SHA256, SHA1, MD5), файл;
— по количеству сущностей: объекты наблюдения, уязвимости, отчеты, вредоносное ПО (далее — ВПО), где:
- объектами наблюдения является вспомогательная сущность (IP, Hash, Domain), не являющаяся индикатором компрометации, но полезная в процессе анализа;
- под уязвимостями подразумеваются сведения об уязвимостях (CVE-идентификатор);
- отчеты представляют под собой PDF-отчеты исследовательских групп о вредоносной активности, объединяющие описательную часть и списки индикаторов;
- ВПО являются сведения о конкретных вредоносных инструментах и компаниях.

— по качественным показателям: теги, дата, связи, где:
- тегами являются выставленные теги у индикатора (tor, shellprobe, …);
- под датой подразумевается наличие данных о времени начала активности, когда активности/времени жизни индикатора [5];
- связи — это наличие связей с другими индикаторами компрометации и сущностями, описание активности, в которой замечен индикатор, или ссылка на внешний отчет.

Выделяются следующие направления назначения TI данных:

— аналитика — предоставляет различные отчеты в PDF-формате, связанные с несколькими типами индикаторов компрометации. Такие отчеты помогают установить принадлежность индикатора компрометации к определенной группировке, определить техники и тактики злоумышленника, предположить дальнейшее развитие атаки или предыдущие шаги;
— алертинг — предоставляет теги в индикаторах компрометации типа IP, что позволяет связывать индикаторы с конкретными уязвимостями и вывести их на непрерывный мониторинг и алертинг;
— обогащение — обогащает весь поток событий данными об активностях, в которых замечены индикаторы, что позволяет дополнить логику правил корреляции [6].

Рассмотрим *реактивные сценарии использования TI данных*, подразумевающие взаимодействие с ними в момент получения индикаторов компрометации в системе:
— сценарий 1 подразумевает отправку TI данных в SIEM. На их основе осуществляется создание правил корреляции, добавление различных уровней доверия. Всю нагрузку и логику работы осуществляет SIEM (рис. 1);

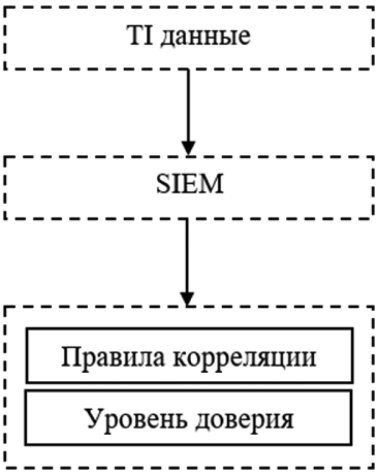

Рис. 1. Сценарий 1 использования TI данных

— сценарий 2 подразумевает отправку TI данных в конечные СЗИ (рис. 2) [7];
— сценарий 3 подразумевает отправку TI данных в TI Platform (далее — TIP) (рис. 3). Данный сценарий в том числе реализует описанные сценарии ранее, т.к. TIP способен отправлять TI данные непосредственно в:
- SIEM, обогащая правила корреляции;
- на конечные СЗИ;
- в SOAR, создавая инциденты ИБ;
- функционал «алертинг» позволяет оперативно оповещать администраторов ИБ об инциденте ИБ.

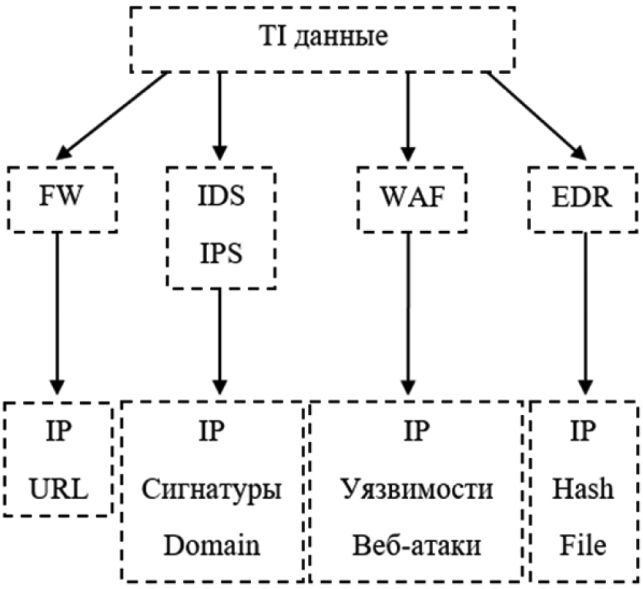

Рис. 2. Сценарий 2 использования TI данных

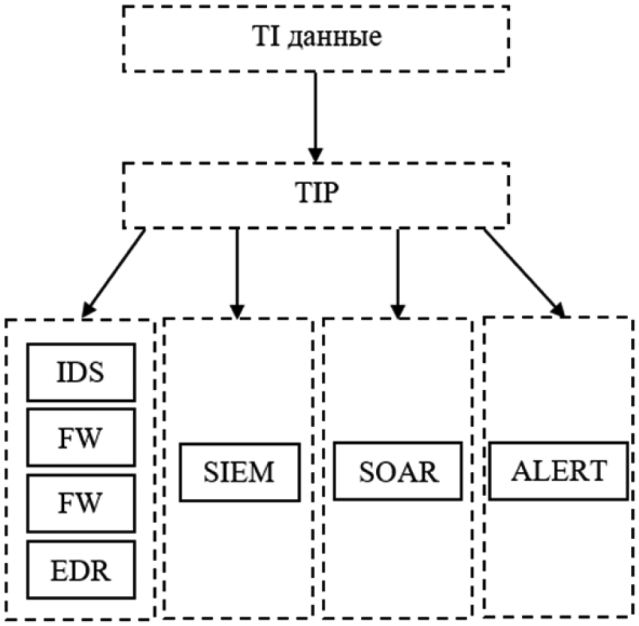

Рис. 3. Сценарий 3 использования TI данных

Продукты TI: краткий обзор

1. RST Cloud Threat Feed, который:
— осуществляет агрегацию и обогащение индикаторов из open-source источников;
— в качестве индикаторов выступают: IP-, URL-адреса, Domain;
— выполняет кросс-корреляцию данных;
— выполняет «умный» скоринг индикаторов;
— реализует быструю интеграцию с SIEM/SOAR/TIP.
2. Kaspersky Threat Intelligence Services, который:
— предоставляет потоки данных об угрозах, отражающих отраслевую специфику (например, для АСУТП);
— предоставляет детальные комплексные и кастомизированные отчеты об угрозах.

3. Group-IB Threat Intelligence & Attribution, который:
— предоставляет аналитику по скомпрометированным аккаунтам;
— предоставляет детальную аналитику по хакерским группировкам;
— предоставляет аналитику по скомпрометированным устройствам (EMEI);
— выполняет графовый анализ.

Автоматизация обработки TI данных

TIP — система, предназначенная для автоматизации обработки TI данных и осуществляющая:

1. сбор данных об угрозах из различных источников;
2. объединение данных в единую систему (агрегация данных);
3. выявление паттернов, трендов, уровень доверия (анализ данных);
4. классификацию угроз по критериям (типу атаки, цели, сектору экономики);
5. распространение через уведомление, отчеты, дашборды;
6. интеграцию с системами обнаружения инцидента, управления уязвимостями, средствами защиты информации, системами мониторинга;
7. автоматическую блокировку IP-адресов, создание правил безопасности, отправку уведомлений (реагирование) [8].

TIP в экосистеме SOC

Поставщики данных поставляют данные в TIP, расположенном в центре SOC. Предложены следующие варианты интеграции (рис. 4) [9]:

1. SIEM:
— отправка индикаторов компрометации непосредственно в SIEM. Всю логику работы осуществляет SIEM;
— сбор индикаторов компрометации из SIEM. Всю логику работы осуществляет TIP.
2. SOAR:
— отправка в SOAR карточек инцидентов и оповещений;
— аналитики информационной безопасности могут загрузить отчет по результату анализа угрозы информационной безопасности в TIP. Таким образом, SOAR будет являться неким поставщиком собственных отчетов, которые будут направляться в TIP. TIP может делиться этими новыми данными в рамках своей Организации [10].
3. Внешние СЗИ — распространение индикаторов компрометации.

Продукты TIP: краткий обзор

1. Kaspersky CyberTrace, который:
— выполняет агрегацию «своих» и «чужих» потоков TI данных;
— реализует возможность заведения пользовательских потоков TI данных;
— предоставляет статистику использования для измерения эффективности используемых потоков TI данных.
2. R-Vision TIP, который:
— реализует интеграцию с ФинЦЕРТ;
— выполняет ретроспективный и проактивный поиск;

Рис. 4. Расположение TIP в экосистеме SOC

— осуществляет формирование собственных бюллетеней угроз и уязвимостей.

Выводы

Авторами проанализирован опыт работы инженеров по информационной безопасности, специализирующихся в области проектирования и внедрения средств мониторинга и реагирования на инциденты ИБ, что позволило обосновать категоризацию и классификацию TI данных, выделить преимущества использования TI данных и определить направления их назначения TI данных, сформировать реактивные сценарии использования TI данных и подход встраивания TIP в экосистему SOC. Приведен краткий обзор TI-решений и TIP-решений.

ЛИТЕРАТУРА

1. Набиуллин, А.А. Применение технологии threat intelligence в информационной безопасности / А.А. Набиуллин, С.Д. Захаров, М.Р. Юсупов // Мавлютовские чтения: материалы XV Всероссийской молодежной научной конференции: в 7 томах, Уфа, 26–28 октября 2021 года. Том 4. — Уфа: Уфимский государственный авиационный технический университет, 2021. — С. 486–494.
2. Лесников, А.Н. Cyber threat intelligence — проактивное обнаружение угроз кибербезопасности / А.Н. Лесников // Информационная безопасность в банковско-финансовой сфере: Сборник научных работ участников ежегодной международной молодежной научно-практической конференции в рамках V Международного форума «Как попасть в пятерку?», Москва, 29 ноября 2018 года. — Москва: Общество с ограниченной ответственностью «Издательство Прометей», 2018. — С. 179–185.
3. Kireev, A.P. Application of Threat Intelligence methods in investigating information security incidents / A.P. Kireev, M.V. Songin // Научные исследования в современном мире. Теория и практика: Сборник избранных статей Всероссийской (национальной) научно-практической конференции, Санкт-Петербург, 10 мая 2021 года. — СПб: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2021. — P. 96–97.
4. Исаков, Н.С. Источники информации об угрозах безопасности информации для Threat Intelligence процесса / Н.С. Исаков, В.Г. Жуков, Д.В. Смирнов // Актуальные проблемы авиации и космонавтики. — 2018. — Т. 2, № 4(14). — С. 224–226.
5. Дрянных, Ю.Ю. Автоматизация сбора, проверки и загрузки индикаторов компрометации в платформу threat intelligence / Ю.Ю. Дрянных, В.Г. Жуков // Актуальные проблемы авиации и космонавтики: Сборник материалов V Международной научно-практической конференции, посвященной Дню космонавтики. В 3-х томах, Красноярск, 08–12 апреля 2019 года / Под общей редакцией Ю.Ю. Логинова. Том 2. — Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2019. — С. 225–227.
6. Бурова, А.В. Threat Intelligence Platform как драйвер автоматизированной информационной безопасности / А.В. Бурова, Ю.А. Матвеева // Цифровизация общества: состояние, проблемы, перспективы: материалы IX Ежегодной Всероссийской научно-практической конференции, Москва, 07 июня 2022 года. Том 1. — Москва: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2022. — С. 158–163.
7. Нурутдинов, А.А. Threat Intelligence в обеспечении информационной безопасности / А.А. Нурутдинов // Молодой исследователь: вызовы и перспективы: сборник статей по материалам CXX международной научно-практической конференции, Москва, 03 июня 2019 года. Том 20 (120). — Москва: Общество с ограниченной ответственностью «Интернаука», 2019. — С. 391–396.
8. Жирнов, В.И. THREAT INTELLIGENCE как основной инструмент предотвращения кибератак / В.И. Жирнов, А.В. Иванов // Современные технологии и автоматизация в технике, управлении и образовании: Сборник трудов II Международной научно-практической конференции, Балаково, 18 декабря 2019 года. Том 1. — Балаково: Национальный исследовательский ядерный университет «МИФИ», 2020. — С. 284–286.
9. Дрянных, Ю.Ю. Структурный подход к расследованию инцидентов информационной безопасности на базе платформы threat intelligence / Ю.Ю. Дрянных, В.Г. Жуков // Решетневские чтения. — 2018. — Т. 2. — С. 324–325.
10. Gupta, S. Cyber security threat intelligence using data mining techniques and artificial intelligence / S. Gupta, A. S. Sabitha, R. Punhani // International Journal of Recent Technology and Engineering. — 2019. — Vol. 8, No. 3. — P. 6133–6140.